CHAPTER 9

Configuring an IP ACL

This chapter describes how to configure IP access control lists (ACLs).

This chapter includes the following sections:

Information About ACLs

An ACL is an ordered set of rules for filtering traffic. When the device determines that an ACL applies to a packet, it tests the packet against the rules. The first matching rule determines whether the packet is permitted or denied. If there is no match, the device applies a default rule. The device processes packets that are permitted and drops packets that are denied. For more information, see the "Implicit Rules" section on page 9-3.

You can use ACLs to protect networks and specific hosts from unnecessary or unwanted traffic. For example, you could use ACLs to disallow HTTP traffic from a high-security network to the Internet. You could also use ACLs to allow HTTP traffic but only to specific sites, using the IP address of the site to identify it in an IP ACL.

This section includes the following topics:

ACL Types and Applications

When a port ACL is applied to a trunk port, the ACL filters traffic on all VLANs on the trunk port.

The following types of port ACLs are supported for filtering Layer 2 traffic:

- IP ACLs—The device applies IPv4 ACLs only to IP traffic.
- MAC ACLs—The device applies MAC ACLs only to non-IP traffic.

Order of ACL Application

ACLs are applied in the following order:

1. Incoming Port ACL
2. Outgoing Port ACL

About Rules

Rules are what you create, modify, and remove when you configure how an ACL filters network traffic. Rules appear in the running configuration. When you apply an ACL to an interface or change a rule within an ACL that is already applied to an interface, the supervisor module creates ACL entries from the rules in the running configuration and sends those ACL entries to the applicable I/O module.

You can create rules in ACLs in access-list configuration mode by using the **permit** or **deny** command. The device allows traffic that matches the criteria in a permit rule and blocks traffic that matches the criteria in a deny rule. You have many options for configuring the criteria that traffic must meet in order to match the rule.

This section describes some of the options that you can use when you configure a rule. For information about every option, see the applicable **permit** and **deny** commands in the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*.

This section includes the following topics:

Source and Destination

In each rule, you specify the source and the destination of the traffic that matches the rule. You can specify both the source and destination as a specific host, a network or group of hosts, or any host. How you specify the source and destination depends on whether you are configuring IP or MAC ACLs. For information about specifying source and destination, see the applicable **permit** and **deny** commands in the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*.

Protocols

IP and MAC ACLs let you to identify traffic by protocol. You can specify some protocols by name. For example, in an IP ACL, you can specify ICMP by name.

You can specify any protocol by number. In MAC ACLs, you can specify protocols by the Ethertype number of the protocol, which is a hexadecimal number. For example, you can use 0x0800 to specify IP traffic in a MAC ACL rule.

In IP ACLs, you can specify protocols by the integer that represents the Internet protocol number. For example, you can use 115 to specify Layer 2 Tunneling Protocol (L2TP) traffic.

For a list of the protocols that each type of ACL supports by name, see the applicable **permit** and **deny** commands in the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*.

Implicit Rules

IP and MAC ACLs have implicit rules, which means that although these rules do not appear in the running configuration, the device applies them to traffic when no other rules in an ACL match. When you configure the device to maintain per-rule statistics for an ACL, the device does not maintain statistics for implicit rules.

All IP ACLs include the following implicit rule that denies unmatched IP traffic:

```
deny ip any any
```

All MAC ACLs include the following implicit rule:

```
deny any any
```

This implicit rule ensures that unmatched traffic is denied, regardless of the protocol specified in the Layer 2 header of the traffic.

Additional Filtering Options

You can identify traffic by using additional options. These options differ by ACL type. The following list includes most but not all additional filtering options:

- IP ACLs support the following additional filtering options:
  - Layer 4 protocol
  - TCP and UDP ports
  - ICMP types and codes
  - IGMP types
  - Precedence level
  - Differentiated Services Code Point (DSCP) value
  - TCP packets with the ACK, FIN, PSH, RST, SYN, or URG bit set
- MAC ACLs support the following additional filtering options:
  - Layer 3 protocol
  - VLAN ID
  - Class of Service (CoS)

For information about all filtering options available in rules, see the applicable **permit** and **deny** commands in the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*.

Sequence Numbers

The device supports sequence numbers for rules. Every rule that you enter receives a sequence number, either assigned by you or assigned automatically by the device. Sequence numbers simplify the following ACL tasks:

- Adding new rules between existing rules—By specifying the sequence number, you specify where in the ACL a new rule should be positioned. For example, if you need to insert a rule between rules numbered 100 and 110, you could assign a sequence number of 105 to the new rule.
- Removing a rule—Without using a sequence number, removing a rule requires that you enter the whole rule, as follows:

  ```
  n1000v(config-acl)# no permit tcp 10.0.0.0/8 any
  ```

  However, if the same rule had a sequence number of 101, removing the rule requires only the following command:

  ```
  n1000v(config-acl)# no 101
  ```

- Moving a rule—With sequence numbers, if you need to move a rule to a different position within an ACL, you can add a second instance of the rule using the sequence number that positions it correctly, and then you can remove the original instance of the rule. This action allows you to move the rule without disrupting traffic.

If you enter a rule without a sequence number, the device adds the rule to the end of the ACL and assigns a sequence number that is 10 greater than the sequence number of the preceding rule to the rule. For example, if the last rule in an ACL has a sequence number of 225 and you add a rule without a sequence number, the device assigns the sequence number 235 to the new rule.

In addition, you can reassign sequence numbers to rules in an ACL. Resequencing is useful when an ACL has rules numbered contiguously, such as 100 and 101, and you need to insert one or more rules between those rules.

Statistics

The device can maintain global statistics for each rule that you configure in IPv4 and MAC ACLs. If an ACL is applied to multiple interfaces, the maintained rule statistics are the sum of packet matches (hits) on all the interfaces on which that ACL is applied.

Note The device does not support interface-level ACL statistics.

For each ACL that you configure, you can specify whether the device maintains statistics for that ACL, which allows you to turn ACL statistics on or off as needed to monitor traffic filtered by an ACL or to help troubleshoot the configuration of an ACL.

The device does not maintain statistics for implicit rules in an ACL. For example, the device does not maintain a count of packets that match the implicit **deny ip any any** rule at the end of all IPv4 ACLs. If you want to maintain statistics for implicit rules, you must explicitly configure the ACL with rules that are identical to the implicit rules. For more information, see the "Implicit Rules" section on page 9-3.

Prerequisites for IP ACLs

IP ACLs have the following prerequisites:

- You must be familiar with IP addressing and protocols to configure IP ACLs.
- You must be familiar with the interface types that you want to configure with ACLs.

Guidelines and Limitations

IP ACLs have the following configuration guidelines and limitations:

- In most cases, ACL processing for IP packets are processed on the I/O modules. Management interface traffic is always processed on the supervisor module, which is slower.
- ACLs are not supported in port channels.

Default Settings

Table 9-1 lists the default settings for IP ACL parameters.

Table 9-1 Default IP ACL Parameters

Parameters	Default
IP ACLs	No IP ACLs exist by default
ACL rules	Implicit rules apply to all ACLs (see the "Implicit Rules" section on page 9-3)

Configuring IP ACLs

This section includes the following topics:

Creating an IP ACL

You can create an IPv4 ACL on the device and add rules to it.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **[no] ip access-list** {*name* | **match-local-traffic**}
3. [*sequence-number*] {**permit** | **deny**} *protocol source destination*
4. **statistics per-entry**
5. **show ip access-lists** *name*
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	**[no] ip access-list** {*name* | **match-local-traffic**} **Example:** n1000v(config)# ip access-list acl-01 n1000v(config-acl)# **Example:** n1000v(config)# ip access-list match-local-traffic n1000v(config-acl)#	Creates the named IP ACL (up to 64 characters in length) and enters IP ACL configuration mode. The **match-local-traffic** option enables matching for locally-generated traffic. The **no** option removes the specified access list.

	Command	Purpose
Step 3	[*sequence-number*] {**permit** | **deny**} *protocol source destination* **Example:** `n1000v(config-acl)# permit ip 192.168.2.0/24 any`	Creates a rule in the IP ACL. You can create many rules. The *sequence-number* argument can be a whole number between 1 and 4294967295. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*.
Step 4	**statistics per-entry** **Example:** `n1000v(config-acl)# statistics per-entry`	(Optional) Specifies that the device maintains global statistics for packets that match the rules in the ACL.
Step 5	**show ip access-lists** *name* **Example:** `n1000v(config-acl)# show ip access-lists acl-01`	(Optional) Displays the IP ACL configuration.
Step 6	**copy running-config startup-config** **Example:** `n1000v(config-acl)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Changing an IP ACL

You can add and remove rules in an existing IPv4 ACL. You cannot change existing rules. Instead, to change a rule, you can remove it and recreate it with the desired changes.

If you need to add more rules between existing rules than the current sequence numbering allows, you can use the **resequence** command to reassign sequence numbers. For more information, see the "Changing Sequence Numbers in an IP ACL" section on page 9-10.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **ip access-list** *name*
3. [*sequence-number*] {**permit | deny**} *protocol source destination*
4. **no** {*sequence-number* | {**permit | deny**} *protocol source destination*}
5. [**no**] **statistics per-entry**
6. **show ip access-list** *name*
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into CLI Global Configuration mode.
Step 2	**ip access-list** *name* **Example:** n1000v(config)# ip access-list acl-01 n1000v(config-acl)#	Places you into IP ACL configuration mode for the specified ACL.
Step 3	[*sequence-number*] {**permit** | **deny**} *protocol source destination* **Example:** n1000v(config-acl)# 100 permit ip 192.168.2.0/24 any	(Optional) Creates a rule in the IP ACL. Using a sequence number allows you to specify a position for the rule in the ACL. Without a sequence number, the rule is added to the end of the rules. The *sequence-number* argument can be a whole number between 1 and 4294967295. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*
Step 4	**no** {*sequence-number* | {**permit** | **deny**} *protocol source destination*} **Example:** n1000v(config-acl)# no 80	(Optional) Removes the rule that you specified from the IP ACL. The **permit** and **deny** commands support many ways of identifying traffic. For more information, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*.
Step 5	[**no**] **statistics per-entry** **Example:** n1000v(config-acl)# statistics per-entry	(Optional) Specifies that the device maintains global statistics for packets that match the rules in the ACL. The **no** option stops the device from maintaining global statistics for the ACL.
Step 6	**show ip access-lists** *name* **Example:** n1000v(config-acl)# show ip access-lists acl-01	(Optional) Displays the IP ACL configuration.
Step 7	**copy running-config startup-config** **Example:** n1000v(config-acl)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Removing an IP ACL

You can remove an IP ACL from the device.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- Make sure that you know whether the ACL is applied to an interface.
- Removing an ACL does not affect the configuration of the interfaces where applied. Instead, the device considers the removed ACL to be empty.

SUMMARY STEPS

1. **config t**
2. **[no] ip access-list** *name*
3. **show ip access-list** *name* **summary**
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**no ip access-list** *name* **Example:** `n1000v(config)# no ip access-list acl-01`	Removes the IP ACL that you specified by name from the running configuration.
Step 3	**show ip access-list** *name* **summary** **Example:** `n1000v(config)# show ip access-lists acl-01 summary`	(Optional) Displays the IP ACL configuration. If the ACL remains applied to an interface, the command lists the interfaces.
Step 4	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Changing Sequence Numbers in an IP ACL

You can change all the sequence numbers assigned to the rules in an IP ACL.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **config t**
2. **resequence ip access-list** *name starting-sequence-number increment*
3. **show ip access-lists** *name*
4. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**resequence ip access-list** *name starting-sequence-number increment* **Example:** `n1000v(config)# resequence access-list ip acl-01 100 10`	Assigns sequence numbers to the rules contained in the ACL, where the first rule receives the starting sequence number that you specify. Each subsequent rule receives a number larger than the preceding rule. The difference in numbers is determined by the increment that you specify. The *starting-sequence-number* argument and the *increment* argument can be a whole number between 1 and 4294967295.
Step 3	**show ip access-lists** *name* **Example:** `n1000v(config)# show ip access-lists acl-01`	(Optional) Displays the IP ACL configuration.
Step 4	**copy running-config startup-config** **Example:** `n1000v(config)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Applying an IP ACL as a Port ACL

Use this procedure to configure a port ACL by applying an IPv4 or ACL to a Layer 2 interface physical port.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You can apply one port ACL to an interface.
- Make sure that the ACL you want to apply exists and that it is configured to filter traffic in the manner that you need for this application. For more information, see the "Creating an IP ACL" section on page 9-6 or the "Changing an IP ACL" section on page 9-7.
- An IP ACL can also be configured in a port profile. For more information, see the "Adding an IP ACL to a Port Profile" procedure on page 9-12.

SUMMARY STEPS

1. **config t**
2. **interface vethernet** *port*
3. **ip port access-group** *access-list* **[in | out]**
4. **show running-config aclmgr**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you into CLI Global Configuration mode.

Step 2	**interface vethernet** *port*
	
	Example:
	`n1000v(config)# interface vethernet 40`
	`n1000v(config-if)#`
		Places you into Interface Configuration mode for the specified vEthernet interface.

Step 3	**ip port access-group** *access-list* [**in** | **out**] **Example:** `n1000v(config-if)# ip port access-group acl-l2-marketing-group in`	Applies an inbound or outbound IPv4 ACL to the interface. You can apply one port ACL to an interface.
Step 4	**show running-config aclmgr** **Example:** `n1000v(config-if)# show running-config aclmgr`	(Optional) Displays the ACL configuration.

	Command	Purpose
Step 5	**copy running-config startup-config** **Example:** `n1000v(config-if)# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Adding an IP ACL to a Port Profile

You can use this procedure to add an IP ACL to a port profile:

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already created the IP ACL to add to this port profile using the "Creating an IP ACL" procedure on page 9-6; and you know its name.
- If using an existing port profile, you have already created it and you know its name.
- If creating a new port profile, you know the interface type (Ethernet or vEthernet) and the name you want to give the profile.
- For more information about port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*;
- You know the name of the IP access control list that you want to configure for this port profile.
- You know the direction of packet flow for the access list.

SUMMARY STEPS

1. **config t**
2. **port-profile** [**type** {**ethernet** | **vethernet**}] *profile-name*
3. **ip port access-group** *name* {**in** | **out**}
4. **show port-profile** [**brief** | **expand-interface** | **usage**] [**name** *profile-name*]
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Description
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Enters global configuration mode.
Step 2	**port-profile** [**type** {**ethernet** | **vethernet**}] *name* **Example:** n1000v(config)# port-profile AccessProf n1000v(config-port-prof)#	Enters port profile configuration mode for the named port profile.
Step 3	**ip port access-group** *name* {**in** | **out**} **Example:** n1000v(config-port-prof)# ip port access-group allaccess4 out	Adds the named ACL to the port profile for either inbound or outbound traffic.
Step 4	**show port-profile name** *profile-name* **Example:** n1000v(config-port-prof)# show port-profile name AccessProf	(Optional) Displays the configuration for verification.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-port-prof)# copy running-config startup-config	(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Applying an IP ACL to the Management Interface

Use this procedure to applying an IPv4 or ACL to the Management interface, mgmt0.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- Make sure that the ACL you want to apply exists and that it is configured to filter traffic in the manner that you need for this application. For more information, see the "Creating an IP ACL" section on page 9-6 or the "Changing an IP ACL" section on page 9-7.

SUMMARY STEPS

1. **config t**
2. **interface mgmt0**
3. **[no] ip access-group** *access-list* **[in | out]**
4. **show ip access-lists** *access-list*
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you into CLI global configuration mode.
Step 2	**interface mgmt0** **Example:** n1000v(config)# interface mgmt0 n1000v(config-if)#	Places you into interface configuration mode for the management interface.
Step 3	**[no] ip access-group** *access-list* [**in** | **out**] **Example:** n1000v(config-if)# ip access-group telnet in n1000v(config-if)#	Applies a specified inbound or outbound IPv4 ACL to the interface. The no option removes the specified configuration.
Step 4	**show ip access-lists** *access-list* **Example:** n1000v(config-if)# show ip access-lists telnet summary IP access list telnet statistics per-entry Total ACEs Configured:2 Configured on interfaces: mgmt0 - ingress (Router ACL) Active on interfaces: mgmt0 - ingress (Router ACL)	(Optional) Displays the ACL configuration.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-if)# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Verifying IP ACL Configurations

To display IP ACL configuration information, use the following commands:

Command	Purpose
show running-config aclmgr	Displays the ACL configuration, including IP ACL configuration and interfaces that IP ACLs are applied to.
show ip access-lists [*name*]	Displays all IPv4 access control lists (ACLs) or a named IPv4 ACL.

Command	Purpose
show ip access-list [*name*] **summary**	Displays a summary of all configured IPv4 ACLs or a named IPv4 ACL.
show running-config interface	Displays the configuration of an interface to which you have applied an ACL.

Monitoring IP ACL

Use the following commands for IP ACL monitoring:

Command	Purpose
show ip access-lists	Displays IPv4 ACL configuration. If the IPv4 ACL includes the **statistics per-entry** command, then the **show ip access-lists** command output includes the number of packets that have matched each rule.
clear ip access-list counters	Clears statistics for all IPv4 ACLs or for a specific IPv4 ACL.

Example Configurations for IP ACL

The following example shows how to create an IPv4 ACL named acl-01 and apply it as a port ACL to vEthernet interface 40:

```
ip access-list acl-01
   permit ip 192.168.2.0/24 any
interface vethernet 40
ip port access-group acl-01 in
```

The following example shows how to enable access list matching for locally-generated traffic:

```
ip access-list match-local-traffic
```

Additional References

For additional information related to implementing IP ACLs, see the following sections:

- Related Documents, page 9-16
- Standards, page 9-16

Related Documents

Related Topic	Document Title
ACL concepts.	*Information About ACLs, page 9-1*
Configuring interfaces.	*Cisco Nexus 1000V Interface Configuration Guide, Release 4.2(1)SV1(4)*
Configuring port profiles.	*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4)*
Complete command syntax, command modes, command history, defaults, usage guidelines, and examples for Cisco Nexus 1000V commands.	*Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for IP ACL

This section provides the IP ACL release history.

Feature Name	Releases	Feature Information
IP ACL for mgmt0 interface	4.2(1) SV1(4)	
IP ACL	4.0(4)SV1(1)	This feature was introduced.